Information Technology Department
Monthly Security Tips
NEWSLETTER

December 2008   Volume 3, Issue 12

Pop-Ups

From ITD Security Section

We've all experienced Pop-up windows, or "pop-ups," while browsing the Internet. Pop-ups may appear without any interaction or prompting by the end user. They can be innocuous, such as when used for advertising, but they can be used for malicious purposes as well. This tip will discuss what pop-ups are and what you can do to keep them from affecting the security of your computer and data.

What are Pop-Ups?

Pop-ups are often used for advertising, to entice you to click on the pop-up ad. Pop-ups can also be used in other ways, such as on a "Help" section of an online form. The pop-up can be read without interfering with the form or page you are already visiting. This technique, for example, could be used on banking or ecommerce sites so as to not interfere with the current transaction or form request.

Occasionally you may encounter a "pop-under" which instead of opening on top of whatever website you are viewing it will open underneath the current web page. That way when you close your browser window you'll be greeted with an unexpected window.

While there are legitimate uses for pop-ups, they can also be used maliciously to entice you to click the pop-up window, which then downloads spyware or malicious code without your knowledge. These kinds of pop-ups often claim to "detect a virus on your computer" or claim to be a "spyware alert!" or offer a "free product" such as laptop or an anti-virus program.

Usually pop-ups are executed through JavaScript, a very popular way of adding content to websites. They can also be executed through online flash programs, though these are more difficult to stop.

What if I encounter pop ups when I am not browsing the Internet?

If you encounter pop-ups, especially an endless stream of them, it is an indication your computer is possibly infected with spyware or a computer virus.

How can you protect yourself against unwanted or malicious pop-ups?

Most Internet browsers include pop-up blockers. They also have a setting to either completely disable JavaScript (and therefore most pop-ups) or to only allow JavaScript with the user's

permission (prompting). Both methods can usually stop advertising and malicious pop-ups. However, sometimes disabling JavaScript (whether via your browser or another program) can interfere with the "look and feel" or even functionality of a legitimate web site.

- Consider using the pop-up blocker function in your browser.

- Consider setting your computer to the "Prompt" setting you before enabling Java scripting.

- Never click inside the pop-up window to close it, even if it has a button or tab that says "Close," "No Thank You," or anything else. Instead, either click on the "X" at the top right corner of the title bar, or depending on your browser or operating system you can hold down the "Alt" key then press "F4" to close the currently opened window.

- Browse as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

- Update your operating system and web browser software.

- Set your browser security to at least "Medium" to help detect unauthorized downloads.

- Use anti-virus and anti-spyware software, and a firewall, and update them all regularly.

For additional information on pop-ups and browser protection, go to:

- Recognizing and Avoiding Spyware: www.msisac.org/awareness/news/2007-06.cfm
- Web Browser Attacks: www.msisac.org/awareness/news/2008-07.cfm
- Browsing Safely: Understanding Active Content and Cookies: www.us-cert.gov/cas/tips/ST04-012.html
- Evaluating Your Web Browser's Security Settings: www.us-cert.gov/cas/tips/ST05-001.html
- Pop-up: http://en.wikipedia.org/wiki/Pop-up
- Spyware: www.onguardonline.gov/topics/spyware.aspx

For more monthly cyber security newsletter tips visit:
http://www.nd.gov/itd/security/newsletters.html

The information provided in the Monthly Security Tips Newsletters is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. Organizations have permission--and in fact are encouraged--to brand and redistribute this newsletter in whole for educational, non-commercial purposes.

Brought to you by:

MS-ISAC

www.msisac.org